



2134
#9

B.M. Jakobsson 15

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): Bjorn Markus Jakobsson
Case: 15
Serial No.: 09/315,628
Filing Date: May 20, 1999
Group: 2134
Examiner: Michael J. Simitoski

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: V. Benavente Date: April 13, 2004

Title: Verification of Correct Exponentiation or Other Operations in Cryptographic Applications

RESPONSE TO OFFICE ACTION

RECEIVED

APR 19 2004

Technology Center 2100

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The remarks below are submitted in response to the first non-final Office Action dated January 15, 2004 in the above-identified application.

REMARKS

The present application was filed on May 20, 1999 with claims 1-27. Claims 1-27 are currently pending in the application. Claims 1, 11 and 22-27 are the independent claims.

In the Office Action, the drawings are objected to under 37 C.F.R. §1.83(a). Moreover, claims 1, 2, 6, 11, 12, 16, 22, 25, 26 and 27 are rejected under 35 U.S.C. §102(b) as being anticipated by "Disavowal protocol for Chaum-van Antwerpen undeniable signature scheme" described in Handbook of Applied Cryptography by Menezes (hereinafter "Menezes"). In addition, claims 3 and 13 are rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes. Furthermore, claim